**PRIVACY AND SECURITY OF**
**PROTECTED HEALTH, CONFIDENTIAL AND SENSITIVE INFORMATION**

The Cabinet for Health Services, in each of its organizational components, and by each of its agents or employees, will act as a responsible steward of all information. The Cabinet will take reasonable and prudent measures to insure the privacy and security of protected health, confidential and sensitive information. All medical information will be handled in accord with applicable law, this includes but is not limited to The Health Insurance Portability and Accountability Act of 1996, other applicable Federal Law, The Kentucky Revised Statutes and the regulations promulgated thereunder. Medical information will only be collected, used, distributed or disclosed for the betterment of public or individual health and in support of the payment, integrity, accountability, reliability, quality and delivery of health services.

At all times, every employee will strive to protect the confidentiality, integrity and accuracy of all information maintained by the Cabinet in any form. It is the **responsibility of** every employee of the Cabinet for Health Services, whether or not they may be a **state merit or non-merit employee, a volunteer, a co-op, an intern, or a contractual entity and its employees** to diligently safeguard protected health, confidential and sensitive information. Each person engaged in the duties of the Cabinet shall be deemed charged with the obligation to comply fully with their assigned tasks but to do so while limiting their access to, and knowledge of, protected health, confidential and sensitive information to the minimum necessary for the accurate and timely completion of their duties.

Protected health, confidential and sensitive information is information that is either protected by law (see "Employee Privacy, Confidentiality and Security Agreement") or is of such personal or private nature that it is normally not treated as public record. **Neither the Cabinet, nor any of its agents or employees will obtain, maintain, release, use, disclose or distribute any information in any form in contravention of currently applicable State or Federal law and the regulations promulgated thereunder. Employees who violate these standards may be subject to progressively severe disciplinary action up to and including suspension or dismissal.**

The Privacy and Security Agreement lists and briefly describes many of the major laws and regulations pertaining to confidential information. There is information not covered specifically by these laws, which is also sensitive and must be safeguarded because of the potential for its misuse. Examples include, but are not limited to the following: social security number, home address, home telephone number, date of birth, height, weight, race, gender, political affiliation, employment history and any other information of a purely personal nature. In addition, a department or office may also have additional requirements necessary to protect information germane to that organizational unit's necessary functions.

## RESPONSIBILITY

An employee's responsibility extends to all situations where employees are accessing, using, circulating, maintaining, disclosing and disposing of reports or documents that contain protected confidential or sensitive information.

Specifically,

1. Employees shall not release, protected health, confidential and sensitive information to themselves or to other persons, entities or employees outside the scope of their duties.

2. Employees shall not seek access to, or inquire about protected health, confidential and sensitive information in excess of the minimum necessary to efficiently discharge responsibilities within the scope of their duties

3. At no time will employees allow the use of their USER ID or Password by another person to access computer data. Allowing access includes but is not limited to leaving a written notation of a USER ID or Password on or near a computer terminal.

4. Employees shall familiarize themselves with the laws pertaining to confidential information described on the revised November 2002 Employee Protected Health, Confidentiality and Security Agreement in order to comply with those restrictions.

5. Employees shall familiarize themselves with what types of information are considered protected health, confidential, personal or sensitive information and do their utmost to protect it. For an example, when documents or reports are circulated that contain such information, the sender will alert the receiver(s) to insure the confidentiality of the data.

6. Employees will not include protected health, confidential, personal or sensitive information on documents or reports if it is not necessary.

7. Employees will not notify directly, or indirectly through third persons, the potential time or occurrence of inspections or surveys of any facility or place of business, that are required by law or regulation to be unannounced, and will otherwise conduct themselves so that any inspection or survey shall be unannounced.

8. Employees when sending mail or other correspondence containing protected health, confidential, personal or sensitive information to any person, the sender will indicate "Personal and Confidential" on the envelope to insure that only the addressee opens it.

9. Employees will take reasonable and appropriate measures to protect identifying numbers. Of particular concern is the social security number because it appears on a myriad of documents and reports, it is one of the most difficult pieces of data to protect but all employees should do their utmost to safeguard it.

10. When no specific guidance is provided regarding responding to requests for information and a written request for information is received, only release the information with the written authorization of the affected party.

11. When no specific guidance is provided regarding responding to an oral or unwritten request for information - where no written request for information is received - only release the information after verifying and documenting the authorization of the affected party.

12. Whenever reasonable and practical, protected health, confidential, personal or sensitive information should not be included on e-mails. (See "the Internet and Electronic Mail" procedure elsewhere in the Procedures Manual.)

13. Whenever reasonable and practical, restricted, protected, internal or privileged reports and documents should be maintained in a secured container.

14. All employees should dispose of documents that contain protected health, confidential, personal or sensitive information correctly. The documents or reports should be placed in a "shred" box that is removed from the work site and destroyed prior to disposal or recycling, rather than placing the documents in a regular solid waste or recycling receptacle.

15. Employees should understand there may be other information that should be protected that is not specifically listed in this procedure or on the "Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement". When in doubt, the employees should consult with their supervisor or the Office of General Counsel at (502) 564-7905 before releasing it.
16. Employees shall not disclose protected health, confidential, personal or sensitive information even after their employment with the Cabinet ceases. State and Federal law regarding protected health, confidential, personal or sensitive information also applies OUTSIDE the employment relationship and criminal or civil penalties including fines and imprisonment could apply.

17. Employees should be aware that **disregard of the privacy and security of protected health, confidential, personal or sensitive information might result in disciplinary action, up to and including dismissal. Additionally, employees may subject themselves to civil and criminal liability for the disclosure of confidential information to unauthorized persons.**

## PROCEDURE FOR "NEW" COMMONWEALTH EMPLOYEES

All new Cabinet employees will be given a copy of this procedure and the revised "Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement" at orientation. The Agreement will be explained fully by the orientation instructor or supervisor before the employee signs it. The Agreement will be placed in the employee's folder in the appropriate Personnel Administrator's Office.

## PROCEDURE FOR "CONTRACTUAL" EMPLOYEES

On the first day of employment, individuals employed contractually will report first to Trinta Cox (for those working in the Human Resources Complex or the Health Services Building), Tresa Straw (for those working in the Fair Oaks Complex) or Jeanette Wilhoite (for those working in the Division of Laboratory Services). Upon arrival, the individual will be asked to read and sign the "Employee Privacy and Security of Protected Health, Confidential and Sensitive Information Agreement". They will then be given a signed memorandum approving them to report for duty to their designated workstation. **Under no circumstances is a supervisor to allow a contractual employee to begin working until a signed memorandum has been presented.**

## PROCEDURE FOR "CURRENT" EMPLOYEES

All current employees will be provided a copy of this procedure and required to sign the "Employee Privacy and Security of Protected Health, Confidential and Sensitive Information

Agreement", which will be placed in their personnel folder in the appropriate Personnel Administrator's Office.

Cabinet for Health Services

# EMPLOYEE PRIVACY AND SECURITY OF PROTECTED HEALTH, CONFIDENTIAL AND SENSITIVE INFORMATION AGREEMENT

PLEASE PRINT:

_____ _____

Last Name, First Name, & M.I. Social Security #

I understand that I may be allowed access to confidential information and/or records in order that I may perform my specific job duties. I further understand and agree that I am not to disclose confidential information and/or records without the prior consent of the appropriate authority(ies) in the Cabinet for Health Services.

I understand that all USERID/Passwords to access computer data are issued on an individual basis. I further understand that I am solely responsible for all information obtained, through system access, using my unique identification. At no time will I allow use of my USERID/Password by any other person.

I understand that accessing or releasing confidential information and/or records, or causing confidential information and/or records to be accessed or released, to myself, other individuals, clients, relatives, etc., outside the scope of my assigned job duties would constitute a violation of this agreement and may result in disciplinary action taken against me, up to and including dismissal. I further understand that employees may subject themselves to civil and criminal liability, as well as disciplinary action, for the disclosure of confidential information to unauthorized persons.

I understand that the following is not an exhaustive list of all confidential information, but is an attempt to include most of the major examples of such information. In the event of doubts about whether certain information is covered by confidentiality requirements, I understand that I should consult my supervisor or the Office of the General Counsel.

Under **KRS 194A.060**, all records and reports of CHS (or CHR) which directly or indirectly identify a patient or client, or former patient or client, of the Cabinet, are confidential.

Under **KRS 216.530** all inspections of long-term care facilities shall be unannounced.

Under **HIPAA**, an individual's health care information must be used by the Cabinet and its employees and agents only for legitimate health purposes like treatment and payment. **45 C.F.R. § 160.101 et seq. and specifically §§ 164.500, 164.501, 164.514** established standards for privacy of health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Health information that must be kept private and secure is called Protected Health Information (PHI). HIPAA establishes in Federal Law the basic principle that an individual's medical records belong to that individual and, with certain exceptions, cannot be used, released or disclosed without the explicit permission of that individual or their legal guardian. This includes disclosing PHI in even casual or informal conversation not related to a legitimate health purpose (like treatment or payment) at any time whether at work or not. HIPAA gives consumers of Cabinet programs and services the right to an explanation of their privacy rights, the right to see their medical records (with some exceptions), the right to request corrections to these records, the right to control the release of information from their records and the right to documented explanations of disclosures by the Cabinet and by others who may have access to this information. Those who violate the rules laid down by HIPAA are subject to federal penalties. For non-criminal **violations of the privacy standards, *including disclosures made in error,*** there are civil monetary penalties of $100 per violation up to $25,000 per year, per standard. Criminal penalties are imposed for violations of the statute that are done knowingly (on purpose) — **up to $50,000 and one year in prison for obtaining or disclosing protected health information; up to $100,000 and up to five years in prison for obtaining or disclosing protected health information under "false pretenses;" and up to $250,000 and up to 10 years in prison for obtaining protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.**

Under **KRS 214.420**, all information in the possession of local health departments or CHS concerning persons tested for, having, or suspected of having sexually transmitted diseases, or identified in an epidemiologic investigation for sexually transmitted diseases, is strictly confidential. A general authorization for the release of medical or other information is not sufficient to authorize release of this information. Breach of this confidentiality is considered a violation under KRS 214.990.

Under **KRS 214.181**, no test results relating to human immunodeficiency virus are to be disclosed to unauthorized persons.

Under **KRS 222.271**, treatment records of alcohol and drug abuse patients are confidential.

Under **KRS 216.2927**, raw data used by the Kentucky Health Policy Board are confidential. This includes data, data summaries, correspondence, or notes that could be used to identify an individual patient, member of the general public, or employee of a health care provider.

Under **KRS 202A.091**, court records relating to hospitalization of the mentally ill are confidential. Violation of the confidentiality of these records is a Class B misdemeanor under KRS 202A.991.

Under **KRS 202B.180**, court records relating to mental retardation admissions are confidential. Violation of the confidentiality of these records is a Class A misdemeanor under KRS 202B.990.

Under **KRS 210.235**, all records which directly or indirectly identify any patient, former patient, or person whose hospitalization has been sought, are confidential.

Cabinet for Health Services

EMPLOYEE PRIVACY AND SECURITY OF PROTECTED HEALTH, CONFIDENTIAL AND SENSITIVE INFORMATION AGREEMENT

Under **KRS 211.902**, the names of individuals are not to be disclosed in connection with lead poisoning records, except as determined necessary by the Cabinet Secretary.

Under **KRS 211.670**, lists maintained by hospitals, and all information collected and analyzed, relating to the Kentucky birth surveillance registry (concerning birth defects, stillbirths, and high risk conditions) are to be held confidential as to the identity of the patient. Violation of this confidentiality is a Class A misdemeanor under KRS 211.991.

Under **KRS 213.131**, unauthorized disclosure or inspection of vital records is unlawful. Violation of the confidentiality laws for vital statistics is a Class B misdemeanor under KRS 213.991.

Under **KRS 434.850**, accessing any computer or computerized information without authorization, or causing any such access without authorization, is a Class A misdemeanor.

Under **KRS 205.8465(4)**, No employee of the state Medicaid Fraud Control Unit, the Office of the Attorney General, the Office of the Inspector General, or the Cabinet for Health Services shall notify the alleged offender of the identity of the person who in good faith makes a report required or permitted by KRS 205.8451 to 205.8483 nor shall the employee notify the alleged offender that a report has been made alleging a violation of KRS 205.8451 to 205.8483 until such time as civil or criminal proceedings have been initiated or a formal investigation has been initiated. Any information or report concerning an alleged offender shall be considered confidential in accordance with the Kentucky Open Records Law, KRS 61.870 to 61.844.

Confidentiality of family planning services is required by **42 C.F.R. § 59. Section 59.11** states: *"All information as to personal facts and circumstances obtained by the project staff about individuals receiving services must be held confidential and may not be disclosed without the individual's consent, except as may be necessary to provide services to the patient or as required by law, with appropriate safeguards for confidentiality. Otherwise, information may be disclosed only in summary, statistical, or other form which does not identify particular individuals."* The confidentiality rules applicable to all programs or projects supported in whole or in part by federal financial assistance, whether by grant or by contract, are found at 42 C.F.R. § 50.310, which states: *"Information in the records or in the possession of programs or projects which is acquired in connection with the requirements of this subpart may not be disclosed in a form which permits the identification of an individual without the individual's consent except as may be necessary for the health of the individual or as may be necessary for the Secretary [of Health and Human Services] to monitor the activities of those programs or projects. In any event, any disclosure shall be subject to appropriate safeguards which minimize the likelihood of disclosures of personal information in an identifiable form."*

Under **42 C.F.R. § 431.305**, the following types of information relating to Medicaid applicants and recipients are confidential: *"(1) Names and addresses; (2) Medical services provided; (3) Social and economic conditions or circumstances; (4) Agency evaluation of personal information; (5) Medical data, including diagnosis and past history of disease or disability; and (6) Any information received for verifying income eligibility and amount of medical assistance payments (see Sec. 435.940ff). Income information received from SSA or the Internal Revenue Service must be safeguarded according to the requirements of the agency that furnished the data. (7) Any information received in connection with the identification of legally liable third party resources under Sec. 433.138 of this chapter."*

I understand that other types of information may also be protected by confidentiality, and that if in doubt as to confidentiality, I should not volunteer information before making certain that the information may be disclosed.

By affixing my signature to this document, I acknowledge that I have been apprised of the relevant laws, regulations, and policies concerning access, use, maintenance, and disclosure of confidential information and/or records which shall be made available to me through my employment in the Cabinet for Health Services. I further agree that it is my responsibility to assure the confidentiality of all information that has been issued to me in confidence even after my employment with the agency has ended.

I have read the above, received a copy of the Cabinet's Confidentiality Policy and understand my responsibilities.

_____ _____

Employee Signature Date

_____ _____

Supervisor Signature Date

_____ _____

Manager, Director, or Commissioner Signature Date

Revised: 11-06-02